

# Investigating the Cost of Anonymity on Dynamic Networks \*

Giuseppe Antonio DI LUNA and Roberto BALDONI

Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti  
Università degli Studi di Roma La Sapienza  
Via Ariosto, 25, I-00185 Roma, Italy  
{baldoni, diluna}@dis.uniroma1.it

## Abstract

In this paper we study the difficulty of counting nodes in a synchronous dynamic network where nodes share the same identifier, they communicate by using a broadcast with unlimited bandwidth and, at each synchronous round, network topology may change. To count in such setting, it has been shown that the presence of a leader is necessary. We focus on a particularly interesting subset of dynamic networks, namely *Persistent Distance* -  $\mathcal{G}(\text{PD})_h$ , in which each node has a fixed distance from the leader across rounds and such distance is at most  $h$ . In these networks the dynamic diameter  $D$  is at most  $2h$ . We prove the number of rounds for counting in  $\mathcal{G}(\text{PD})_2$  is at least logarithmic with respect to the network size  $|V|$ . Thanks to this result, we show that counting on any dynamic anonymous network with  $D$  constant w.r.t.  $|V|$  takes at least  $D + \Omega(\log |V|)$  rounds where  $\Omega(\log |V|)$  represents the additional cost to be payed for handling anonymity. At the best of our knowledge this is the first non trivial, i.e. different from  $\Omega(D)$ , lower bounds on counting in anonymous interval connected networks with broadcast and unlimited bandwidth.

---

\*A shorter version of this manuscript has appeared as brief announcement at PODC 2015.

# 1 Introduction

Computing over a dynamic distributed system has become mainstream in the recent years, this has been due to advent of peer-to-peer systems, the capillary distribution of mobile devices and growing impact of sensors networks. Such technologies force the designer of distributed systems to think about the dynamicity as a fundamental and persistent property of the system that is present during the entire system lifetime.

As in [5, 8, 9, 14, 17], in this paper we consider systems where processes are stable (i.e., the set  $|V|$ ) while there is an adversary that continuously changes the underlying communication graph connecting such processes. The adversary can be either fair or worst-case. A fair adversary creates or removes edges from the communication graph following a strategy that does not aim to violate the correctness of the distributed algorithm (e.g., random strategy). This is the typical dynamic behavior exhibited by a peer to peer system [8, 14]. A *worst-case adversary* continuously changes the underline communication graph, having access to nodes' local variables, in order to deploy at *each computational round* the worst possible network topology to contrast the correctness of the algorithm. The adversary is constrained to maintain in each round a connected topology, i.e. 1-interval connectivity property [9].

*We investigate the difficulty of counting the network size under a worst-case adversary, where anonymous nodes communicate any amount of data among each other by using an anonymous broadcast.* Solving the counting problem is of primary importance since it may be seen as a basic building block necessary, for example, to compute generic aggregated function. It has been shown in [15] that counting cannot be solved without a leader and several counting algorithms have been provided in the last couple of years that minimize the knowledge about the adversary that nodes need in order to count (e.g., [13]). However, at the best of our knowledge there is no study that addresses the actual cost of anonymity in terms of time necessary to output the number of processes that form the computation and no trivial lower bound, i.e. different from  $\Omega(D)$ , is known for such environment.

To study this cost, we first identify an interesting family of subsets of dynamic graphs, namely  $\mathcal{G}(\text{PD})_h$  graphs. In such graphs each node has a persistent distance from the leader across rounds and such distance is at most  $h$ . It is easy to see that graphs in  $\mathcal{G}(\text{PD})_1$  are actually star graphs with the leader at the center and that the adversary cannot change any of such graphs without compromising the connectivity of the graph itself. In such a scenario the leader is able to output the exact count in one round independently of the anonymity of the processes.

Let us now consider  $\mathcal{G}(\text{PD})_2$ , processes at distance 2 are connected to the leader by an unknown number of paths that dynamically changes at each round. If nodes are anonymous, ambiguity is created among these multiple dynamic paths. To overcome such ambiguity, the leader will need more than 2 rounds <sup>1</sup>. For such family of graphs we show a lower bound,  $\Omega(\log |V|)$ , on the number of rounds necessary to solve the counting problem. This result is proved by showing that counting in a dynamic labeled multigraph where nodes are directly connected to the leader is at most as difficult as counting in  $\mathcal{G}(\text{PD})_2$ . Then we prove the bound on such dynamic multigraphs by using linear algebra techniques.

The rest of the paper is structured as follows: Section 2 presents the related work; Section 3 defines the system model; Section 4 shows the bound on  $\mathcal{G}(\text{PD})_2$ . Section 5 concludes the paper.

## 2 Related Work

The question concerning what can be computed on top of static anonymous networks, has been pioneered by Angluin in [2] and by Yamashita and Kameda [18]. In the domain of non-anonymous dynamic networks the counting problem has been addressed in the following contexts: (i) dynamicity governed by node churn in the context of distributed query execution [3, 4], (ii) dynamicity governed by random adversary in the context of peer-to-peer networks [14] and (iii) dynamicity governed worst-case adversary in the context of 1-interval connectivity [9, 17].

---

<sup>1</sup>Solutions exploiting randomness (i.e. tossing coins hoping for different outcomes) are not viable, since we assume the source of randomness available to processes is governed by the worst case adversary.

**Counting in anonymous dynamic networks:** In [8], the authors propose a gossip-based protocol to compute aggregation function in a dynamic network by exploiting an invariant, called *conservation of mass*, defined over the whole set of processes. The network graph considered by [8] is governed by a fair random adversary. The first work investigating the problem of counting in an anonymous network with worst-case adversary is [15]. The authors provided an algorithm that, under the assumption of a fixed upper bound on the maximum node degree, it computes an upper bound on the size of the network. Building on this result, [12] proposes an exact counting algorithm under the same assumption. Finally, [13] provides a counting algorithm for 1-interval connected networks considering each node is equipped with a local degree detector, i.e. an oracle able to predict the degree of the node in each graph generated by the adversary. Both [12] and [13] terminate in an exponential number of rounds.

**Bounds on adversarial-based dynamic networks:** A fundamental problem that is correlated with counting in dynamic networks with IDs is the  $k$  tokens dissemination, defined as follows [9]: each token is initially owned by a node belonging to  $V$ , then processes exchange tokens, the  $k$  tokens dissemination terminates when all  $k$  tokens have been received by each node in  $V$ . [9] proved that when each node may send only one token at each round any  $k$  token dissemination algorithm based on token forwarding<sup>2</sup> terminates in  $\Omega(|V|\log k)$  round. In [6], the authors improved the bound to  $\Omega(\frac{|V|k}{\log |V|})$ . Starting from these results, [7] provides bounds for different adversarial-based dynamic networks. It is well known that in network with IDs  $n$  (all-to-all) token dissemination solves counting [1]. In the same paper, it is introduced a connection between two-party token dissemination, a variant of  $k$ -token dissemination, and the counting problem. The authors show a lower bound for the two-party problem is also a lower bound for counting. In anonymous dynamic networks considered in [1],  $k$ -token dissemination can be solved by a trivial flooding algorithm in  $\mathcal{O}(D)$  rounds. Finally, [10] shows that in directed static network with IDs and limited bandwidth, the number of rounds needed to solve counting is function of the network size even when  $D = 2$ .

### 3 Model of the computation

We consider a synchronous distributed system composed by a finite static set of processes  $V$  (also called *nodes*). Nodes in  $V$  are *anonymous*, i.e., they initially have no identifiers and execute a deterministic *round-based* computation. Processes communicate through a communication network which is *dynamic*. We assume at each round  $r$  the network is stable and represented by a graph  $G_r = (V, E(r))$  where  $V$  is the set of nodes and  $E(r)$  is the set of bidirectional links at round  $r$  connecting processes in  $V$ .

**Definition 1.** A dynamic graph  $G = \{G_0, G_1, \dots, G_r, \dots\}$  is an infinite sequence of graphs one at each round  $r$  of the computation.

The neighborhood of a node  $v$  at round  $r$  is denoted by  $N(v, r) = \{v' : \{v', v\} \in E(r)\}$ . Given a round  $r$  we denote with  $p_{v,v'}$  a path on  $G_r$  between  $v$  and  $v'$ . Moreover we denote with  $P(r)_{v',v}$ , the set of all paths between  $v, v'$  on graph  $G_r$ . The distance  $d_r(v', v)$  is the minimum length among the lengths of the paths in  $P(r)_{v',v}$ , the length of the path is defined as the number of edges.

Computation proceeds by rounds. Every round is divided in a *send phase* where processes send the messages for the current round and a *receive phase* where nodes process received messages and prepare those that will be sent in the next round. Processes communicate with its neighbors through an *anonymous broadcast* primitive: a message  $m$  sent by node  $v_i$  in the send phase of round  $r$  will be delivered to all its neighbors during the receive phase of  $r$ . Let us remark that in such model a node does not know the value  $|N(v, r)|$  before the receive phase of round  $r$ .

Let us define the dynamic diameter  $D$  of dynamic graph  $G$ . A node  $v$  floods message  $m$  by broadcasting it at each round, each process receiving a flooded message  $m$  starts, in its turn, a flooding of  $m$ . The flood of  $m$  terminates when it has been received by all nodes. A network has a dynamic diameter  $D$  if for any  $v$  and for any round  $r$  the flood of a message that starts at round  $r$

<sup>2</sup>Token-forwarding algorithms are not allowed to combine, split, or change tokens in any way [7].

from node  $v$  terminates at most by round  $r + D$ . Intuitively the dynamic diameter is the maximum time needed to disseminate messages to all nodes in the network. In this work we consider networks where  $D$  is fixed and constant with respect to  $|V|$ .

**Leader-based computation and worst case adversary** We assume the selection of a topology graph at round  $r$  is done by an omniscient adversary that may choose at each step the worst configuration to challenge a counting algorithm. Due to the impossibility result shown in [15], we assume any counting algorithm that works over a dynamic graph has a leader node  $v_l$  starting with a different unique state w.r.t. all the other nodes.

**Definition 2.** *Given a dynamic network  $G$  with  $|V|$  processes, a distributed algorithm  $\mathcal{A}$  solves the counting on  $G$  if it exists a round  $r$  at which the leader outputs  $|V|$  and terminates.*

**Persistent distance dynamic graphs** Let us characterize dynamic graphs according to the distances among a node  $v$  and the leader  $v_l$ .

**Definition 3.** *(Persistent Distance over  $G$ ) Let us consider a dynamic graph  $G$ . The persistent distance between  $v$  and  $v_l$  over  $G$ , denoted  $D(v, v_l) = d$ , is defined as follow:  $D(v, v_l) = d$  iff  $\forall r, d_r(v, v_l) = d$ .*

Let us now introduce a set of dynamic graphs based on the distance between the leader and the nodes of a graph.

**Definition 4.** *(Persistent Distance set) A graph  $G$  belongs to Persistent Distance set, denoted  $\mathcal{G}(\text{PD})$ , iff  $\forall v \in G, \exists d \in \mathbb{N}^+ :: D(v, v_l) = d$*

**Graphs in  $\mathcal{G}(\text{PD})_2$**  Among the dynamic graphs belonging to  $\mathcal{G}(\text{PD})$  we can further consider the set of graphs, denoted  $\mathcal{G}(\text{PD})_h$ , whose nodes have maximum distance  $h$  from the leader with  $1 < h \leq |V|$ . Thus, given a graph in  $\mathcal{G}(\text{PD})_h$  we can partition its nodes in  $h$  sets,  $\{V_0, V_1, \dots, V_h\}$ , according to their distance from the leader. The focus of this paper is on dynamic graphs belonging to  $\mathcal{G}(\text{PD})_2$ . As an example, figure 1 depicts a graph belonging to  $\mathcal{G}(\text{PD})_2$  at round 0, 1 and 2 whose dynamic diameter is  $D = 4$ . If node  $v_0$  starts a flood at round 0, this flood will indeed reach node  $v_3$  at round 3. The task of the leader node  $v_l$  is to count nodes in  $V_2$ .

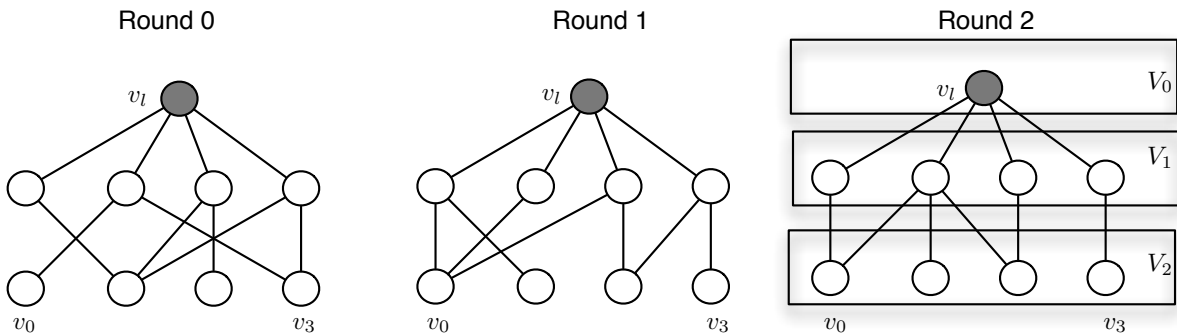


Figure 1: An example of a graph belonging to  $\mathcal{G}(\text{PD})_2$  along three rounds

## 4 Lower bound for $\mathcal{G}(\text{PD})_2$

In this section we consider the  $\mathcal{G}(\text{PD})_2$  set and compute a lower bound for counting time. This is done by introducing a *Dynamic Bipartite Labeled  $k$ -Multigraphs* ( $\mathcal{M}(\text{DBL}_k)$ ), by showing that counting on  $\mathcal{G}(\text{PD})_2$  requires at least the same number of rounds as counting over  $\mathcal{M}(\text{DBL}_k)$  and by finally showing a lower bound on the number of rounds needed to count over  $\mathcal{M}(\text{DBL}_k)$ .

#### 4.1 Counting in Dynamic Bipartite Labeled $k$ -Multigraphs ( $\mathcal{M}(\text{DBL}_k)$ )

Let consider a dynamic connected multigraph  $M$  defined as follows  $M = \cup_{r=0}^{\infty} \{(\{v_l\} \cup W, E(r), f_r, l_r)\}$  where  $E(r)$  is a set of edges at round  $r$ ,  $W$  a set of nodes,  $f_r : E(r) \rightarrow \{v_l\} \times W$  a function that maps each edge to the endpoints nodes and  $l_r : E(r) \rightarrow \{1, 2, \dots, k\}$  a function labeling edges.  $M$  belongs to  $\mathcal{M}(\text{DBL}_k)$  if for each round  $r$  the number of edges connecting a node  $v \in W$  to  $v_l$  is less than  $k + 1$ , more formally  $\forall r, \forall v \in W, E^v(r) = f_r^{-1}(v_l, v) :: 1 \leq |E^v(r)| \leq k$ ; Given  $e', e'' \in E^v(r)$  we have  $l_r(e') \neq l_r(e'')$ , that is if two edges  $e', e''$  share the same non leader node as endpoint they must have different label, as example see edges that involve node  $v$  in Figure 2. For simplicity we will refer as  $M_r$  the instance of  $M$  at round  $r$ . Figure 2 shows an example of a dynamic connected multigraph  $M$  at round  $r$  belonging to  $\mathcal{M}(\text{DBL}_3)$ . We assume that when a node  $v \in \{v_l\} \cup W$  receives a message from a node  $w$  at round  $r$  by edge  $e$ , it also obtains the label  $l_r(e)$ .

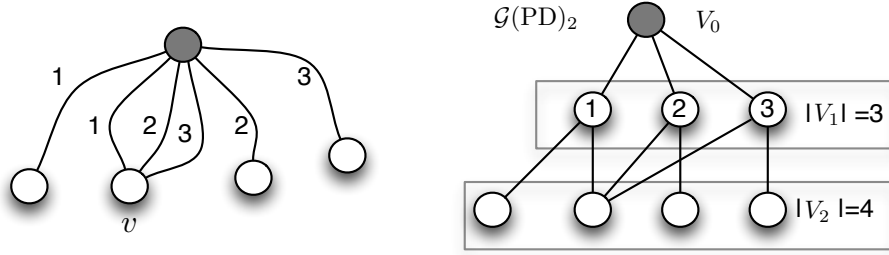


Figure 2: Trasformation, at round  $r$ , from  $\mathcal{M}(\text{DBL}_3)$  multigraph to  $\mathcal{G}(\text{PD})_2$ .

**Lemma 1.** *Let us consider a dynamic connected multigraph  $M$  in  $\mathcal{M}(\text{DBL}_k)$ . If any counting algorithm based on message passing takes more than  $T$  rounds to complete on  $M$ , then there exists a graph  $G$  in  $\mathcal{G}(\text{PD})_2$  such that any counting algorithm based on message passing requires more than  $T$  rounds to complete on  $G$ .*

*Proof.* From  $M_r = (\{v_l\} \cup W, E(r), f_r, l_r)$  we build an instance  $G_r^{id} = (V = \{(V_0 = \{v_l\}) \cup V_1 \cup (V_2 = W)\}, E_{id}(r))$  belonging to  $G^{id} \in \mathcal{G}(\text{PD})_2$  such that  $V_1$  contains  $k$  nodes having unique identifiers in  $[1, \dots, k]$ ,  $V_0$  contains only the leader node  $v_l$  and the set of nodes  $V_2 = W$ . Additionally, at round  $r$  we have that  $\exists e : (v, w) \in E_{id}(r)$  with  $v \in V_1$  and  $w \in V_2$  where  $id(v) = j$  if and only if  $\exists e' \in E(r)$  with  $f_r(e') = (v_l, w), l_r(e') = j$  with  $w \in W$ . Figure 2 shows the transformation at round  $r$  between a dynamic graph in  $\mathcal{M}(\text{DBL}_3)$  and one in  $\mathcal{G}(\text{PD})_2$ . Let us notice that the node with label 1 in  $V_1$  at each  $G_r^{id}$  is connected to the nodes in  $V_2$  that correspond to nodes in  $W$  that are connected in  $M_r$  to  $v_l$  by edges labeled with 1. As a consequence, the leader  $v_l$  in  $M$  is actually the union of local memories of processes in  $\{v_l\} \cup V_1$  in  $G^{id}$ . Let us assume that there not exist a message passing algorithm solving the counting problem in  $M$  with  $T$  rounds, then it is not possible to count nodes in  $V_2$  on  $G^{id}$  in  $T$  rounds even by merging the memories of  $\{v_l\} \cup V_1$ , by knowing the size  $k$  of  $V_1$  and by having unique IDs for nodes in  $V_1$ . Consider now the dynamic graph  $G$  derived by  $G^{id}$  removing the identifiers of nodes in  $V_1$ . Counting nodes in  $G$  is at least as hard as counting nodes in  $G^{id}$ . As an example, without identifiers the leader cannot realize if messages of two successive rounds arrive from the same node of  $V_1$ . Thus it is not possible for the leader to count the size of  $G$  in less than  $T$  rounds.  $\square$

From the lemma follows that a lower bound for counting on  $\mathcal{M}(\text{DBL}_k)$  holds also for graphs in  $\mathcal{G}(\text{PD})_2$ . Now we introduce some definitions on  $M$ . Let consider an instance  $M$  of the family  $\mathcal{M}(\text{DBL}_k)$ .

**Definition 5.** (Set of edge labels of a node at round  $r$ ) Given a node  $v \in W$  at round  $r$  we define the set of edge labels  $L(v, r) : \{l_1, \dots, l_j\}$  with  $l_i \in L(v, r)$  iff  $\exists e \in E(r)$  and  $l_r(e) = l_i$  and  $f_r(e) = (v, v_l)$ .

As an example in Figure 2, the edge label set of node  $v$  at round  $r$  is  $\{1, 2, 3\}$ .

**Definition 6.** (State of a non-leader process) Given a node  $v \in W$  at round  $r$ , we define the state  $S(v, r)$  as an ordered list  $S(v, r) : [(\perp), L(v, 0), \dots, L(v, r-1)]$  where  $(\perp)$  is the first state of any non-leader node<sup>3</sup>.

Given a list  $A : [L_0, L_1, \dots, L_{r-1}]$  we have that  $|A|$  denotes the number of nodes with the same state  $S(v, r) = A$  at round  $r$ . Ref. Figure 1: we have  $S(v, r+1) = [\perp, \dots, \{1, 2, 3\}]$  and  $|S(v, r+1)| = 1$  since  $v$  is the only node connected to  $v_l$  by  $\{1, 2, 3\}$  at round  $r$ .

**Definition 7.** (State of a leader node at round  $r$ ) Given the leader  $v_l$  at round  $r$  we define the leader state  $S(v_l, r)$  as  $[C(v_l, 0), \dots, C(v_l, r-1)]$  where  $C(v_l, i)$  with  $i < r$  is a multiset of elements,  $(j, S(v, i)) \in C(v_l, i)$  iff it exists a node  $v$  with state  $S(v, i)$  connected to  $v_l$  by an edge with label  $j$ .

As for states of local nodes,  $|(j, S(v, r))|$  denotes the number of nodes with state equal to  $S(v, r)$  connected to  $v_l$  by an edge with label  $j$  at round  $r$ . Let us remark that the state of the leader  $v_l$  can be constructed by a simple message passing protocol where at each round each node sends to the leader its own state and where the leader node sends just a dummy message.

## 4.2 Lower Bound for $\mathcal{M}(\text{DBL}_k)$

We introduce some notation on vectors and matrices used in this section.

**Linear algebra notation** Given a vector  $\mathbf{a} \in \mathbb{Z}^n$ , we denote as  $(\mathbf{a})_j$  the  $j$ -th component of  $\mathbf{a}$  (with  $1 \leq j \leq n$ ) and as  $\sum \mathbf{a}$  the sum of all components of  $\mathbf{a}$ . Additionally,  $\sum^+ \mathbf{a}$  (resp.  $\sum^- \mathbf{a}$ ) denotes the sum of only the positive (resp. negative) components of  $\mathbf{a}$ . Given two vectors  $\mathbf{a}, \mathbf{b}$  we have  $\begin{bmatrix} \mathbf{a} \\ \mathbf{b} \end{bmatrix}$  is the vector obtained by appending the elements of the vector  $\mathbf{b}$  after the last element of vector  $\mathbf{a}$ . Given a matrix  $\mathbf{M} \in \mathbb{Z}^{n,m}$  we denote with  $(\mathbf{M})_j$  its  $j$ -th row (with  $1 \leq j \leq n$ ) and we denote as  $\ker(\mathbf{M})$  the set of vectors  $\mathbf{a} \in \mathbb{Z}^m$  such that  $\mathbf{M}\mathbf{a} = \mathbf{0}$ . We also consider the set of vectors  $B = \{\mathbf{a}^1, \dots, \mathbf{a}^\ell\}$  that form a basis for  $\ker(\mathbf{M})$ , i.e.,  $\ker(\mathbf{M}) = \text{SPAN}(B)$ . Finally we denote as  $\mathbf{a}_r$  the instance of vector  $\mathbf{a}$  at round  $r$ .

We prove the bound for the family  $\mathcal{M}(\text{DBL}_k)$  by first proving the lower bound for  $\mathcal{M}(\text{DBL}_2)$ . Considering the latter proof, we first introduce a system of equations that characterizes the states of the nodes of the multigraph at round zero. The lower bound for  $\mathcal{M}(\text{DBL}_2)$  is then proved by studying the evolution of this system of equations through the rounds.

**Consider  $M \in \mathcal{M}(\text{DBL}_2)$  and  $r = 0$ :** At the end of round 0 the leader has state  $S(v_l, 0) : [\{(1, [\perp]), (2, [\perp])\}]$ , this leader state can be generated by many different configurations of nodes and edges in  $M$ . Such configurations are determined by the number of non leader processes with states  $\{\{1\}\}, \{\{2\}\}, \{\{1, 2\}\}$  and they are solutions of the following system of equations at round 0:

$$\begin{cases} |(1, [\perp])| = |\{\{1\}\}| + |\{\{1, 2\}\}| \\ |(2, [\perp])| = |\{\{2\}\}| + |\{\{1, 2\}\}| \end{cases} \quad (1)$$

$r=0$

with the additional constraint that any variable in the solution cannot assume a negative value. When the leader updates its state, in successive rounds, we have a new system of equations. The system of equations 1 can be written in a matrix form as follows:

$$\mathbf{m}_0 = \mathbf{M}_0 \mathbf{s}_0 \quad (2)$$

where  $\mathbf{M}_0 : \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$  represents the matrix of coefficients of the system at round 0,  $\mathbf{m}_0$  is the column vector of constant terms (each component of  $\mathbf{m}_r$  represents the multiplicity of a certain element in the state of the leader at round  $r$ ) and  $\mathbf{s}_0$  is a solution vector. Let us remark that  $\mathbf{M}_r$  depends of the

<sup>3</sup>For simplicity whenever not necessary we omit the presence of  $(\perp)$  as first element of  $S(v, r)$ .

round only while  $\mathbf{m}_r$  depends of the leader state at round  $r$ . As a consequence  $\mathbf{M}_r$  characterizes any multigraph of the family  $\mathcal{M}(\text{DBL}_2)$ .

The matrix  $\mathbf{M}_0$  is characterized by  $\ker(\mathbf{M}_0) = \text{SPAN}(\mathbf{k}_0 : [1 \ 1 \ -1]^\top)$ . Solutions of the matrix equation 2 are related by the following linear combination with the kernel vector  $\mathbf{k}_0$ :  $\mathbf{s}'_0 = \mathbf{s}_0 + t\mathbf{k}_0$  with  $t \in \mathbb{N}$  and such that each component of  $\mathbf{s}'_0$  is non negative. As a consequence, given  $\mathbf{m}_0$  the possible solutions of (1) are restricted to a finite discrete set of points over a segment with direction  $\mathbf{k}_0$ . From the point of view of the leader each solution represents a distinct graph belonging to  $\mathcal{M}(\text{DBL}_2)$  with a different number of processes:  $\sum \mathbf{s}'_0 - \sum \mathbf{s}_0 = t \sum \mathbf{k}_0 = t$ .

Considering the example of Figure 3, the system of equations at round 0 for the multigraph  $M$  is the following

$$\begin{cases} 2 = |[\{1\}]| + |[\{1, 2\}]| \\ 2 = |[\{2\}]| + |[\{1, 2\}]| \end{cases}_{r=0} \quad (3)$$

where  $\mathbf{m}_0 : [2 \ 2]^\top$ . For such system of equations a solution is  $\mathbf{s}_0 : [0 \ 0 \ 2]^\top$ , then using the kernel transformation another solution is  $\mathbf{s}'_0 = \mathbf{s}_0 + 2\mathbf{k}_0 : [2 \ 2 \ 0]^\top$ , these two solutions correspond to two  $M, M' \in \mathcal{M}(\text{DBL}_2)$  of different size that generate the same state  $S(v_l, 0)$  as depicted in Figure 3. These two graphs are indistinguishable from the leader at round 0 thus the leader is not able to output a correct count.

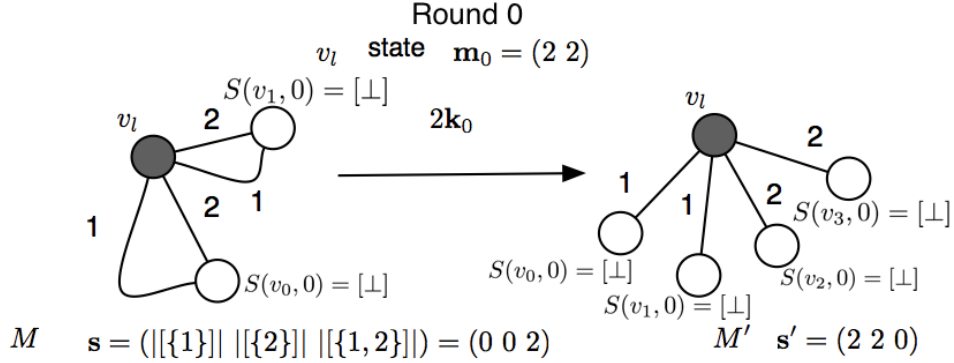


Figure 3: Two dynamic multigraphs  $M, M' \in \mathcal{M}(\text{DBL}_2)$  of different size that are indistinguishable at round  $r = 0$ , the relationship among  $M, M'$  is given by the kernel vector  $\mathbf{k}_0$

The idea that we will use to show the lower bound is to characterize how the kernel space of  $\mathbf{M}_r$  evolves and under which condition of the kernel space we have an unique solution, that corresponds to an unique size  $|W|$ .

**General structure of  $\mathbf{M}_r$ .** At round  $r$ , the system of equations becomes  $\mathbf{m}_r = \mathbf{M}_r \mathbf{s}_r$ . The number of columns of  $\mathbf{M}_r$  is equal to the number of all possible states of non-leader nodes, at round  $r + 1$ , which is  $\text{column}(r) = 3^{r+1}$ . Each row of  $\mathbf{M}_r$  corresponds to a possible connection  $(j, S(v, r'))$  of  $v_l$  at some round  $0 \leq r' \leq r$ . Thus the number of rows at round  $r$  is two times the number of existent states in  $[0, r]$ :  $\text{row}(r) = 2 \sum_{k=0}^r 3^k$ .

As an example, at the end of round 1, the system contains 8 equations ( $2 \cdot 3^0 + 2 \cdot 3^1$ ) and 9 variables (i.e.  $3^2$  rows) and the associated matrix  $\mathbf{M}_1$  are:

$$\begin{cases}
|(1, [\perp])| = \sum_{j \in \{\{1\}, \{2\}, \{1,2\}\}} |[\{1\}, j]| + \sum_{j \in \{\{1\}, \{2\}, \{1,2\}\}} |[\{1,2\}, j]| \\
|(2, [\perp])| = \sum_{j \in \{\{1\}, \{2\}, \{1,2\}\}} |[\{2\}, j]| + \sum_{j \in \{\{1\}, \{2\}, \{1,2\}\}} |[\{1,2\}, j]| \\
|(1, \{\{1\}\})| = |[\{1\}, \{1\}]| + |[\{1\}, \{1,2\}]| \\
|(1, \{\{2\}\})| = |[\{2\}, \{1\}]| + |[\{2\}, \{1,2\}]| \\
|(1, \{\{1,2\}\})| = |[\{1,2\}, \{1\}]| + |[\{1,2\}, \{1,2\}]| \\
|(2, \{\{1\}\})| = |[\{1\}, \{2\}]| + |[\{1\}, \{1,2\}]| \\
|(2, \{\{2\}\})| = |[\{2\}, \{2\}]| + |[\{2\}, \{1,2\}]| \\
|(2, \{\{1,2\}\})| = |[\{1,2\}, \{2\}]| + |[\{1,2\}, \{1,2\}]|
\end{cases} \quad (4) \quad \mathbf{M}_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (5)$$

Let us now consider how it is built the equation at round  $r$  derived from the generic leader connection  $(j, [x_0, \dots, x_{r'-1}])$  with  $j \in \{1, 2\}$  introduced at round  $r'$  in the system of equations, i.e.,  $|(j, [x_0, \dots, x_{r'-1}])| = |[x_0, \dots, x_{r'-1}, \{j\}]| + |[x_0, \dots, x_{r'-1}, \{1, 2\}]|$ . This equation at round  $r$  becomes:

$$|(j, [x_0, \dots, x_{r'}])| = \sum_{\forall s \in (\{\{1\}\}|\{\{2\}\}|\{\{1,2\}\})^{r-r'}} |[x_0, \dots, x_{r'-1}, \{j\}, s]| + \sum_{\forall s \in (\{\{1\}\}|\{\{2\}\}|\{\{1,2\}\})^{r-r'}} |[x_0, \dots, x_{r'-1}, \{1, 2\}, s]|$$

where  $(\{\{1\}\}|\{\{2\}\}|\{\{1,2\}\})^{r-r'}$  is the set of all possible lists with elements in  $\{\{1\}, \{2\}, \{1, 2\}\}$  and size  $r - r'$ . As an example see the equation associated with  $|(1, [\perp])|$  at round 0 (see Equation 1) and the equation associated with  $|(1, [\perp])|$  at round 1 (see Equation 4).

Let notice  $\ker(\mathbf{M}_1) = \{\mathbf{k}_1 = [1 \ 1 \ -1 \ 1 \ 1 \ -1 \ -1 \ -1 \ 1]^T\}$ , thus we have  $\langle \mathbf{k}_1 \rangle = 1$  with  $\langle \mathbf{k}_1 \rangle^+ = 5$ ,  $\langle \mathbf{k}_1 \rangle^- = 4$ . Now let us consider a solution  $\mathbf{s}_1$  with  $\langle \mathbf{s}_1 \rangle \leq 3$ . It is easy to see that  $\mathbf{s}'_1 = \mathbf{s}_1 + t\mathbf{k}_1$  has at least one negative component for any  $t \neq 0$ : since  $\langle \mathbf{k}_1 \rangle^- = 4$  is not possible to have a solution  $\mathbf{s}_1$  that as at least one unitary component for each negative component of  $\mathbf{k}_1$ . Thus  $\mathbf{s}'_1$  cannot be a solution that represents a dynamic multigraph.

This means that if  $n \leq 3$  is possible to obtain the count in 2 rounds, since there is only one possible solution of the system of equations for any  $\mathbf{m}_1$  generated by a multigraph with  $n \leq 3$ . For  $n \geq 4$  we have at least two possible solutions of different size, i.e. we have  $\mathbf{s}_1 = [0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0]^T$  with  $n = 4$  processes and  $\mathbf{s}' : [1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1]^T = \mathbf{s}_1 + \mathbf{k}_1$  with  $n = 5$ . It is easy to check that  $\mathbf{m}_1 = \mathbf{M}_1 \mathbf{s}_1 = \mathbf{M}_1 \mathbf{s}'_1$ , thus we have two multigraphs of different sizes that generate the same state  $\mathbf{m}_1$  at  $v_l$ , see Figure 4.

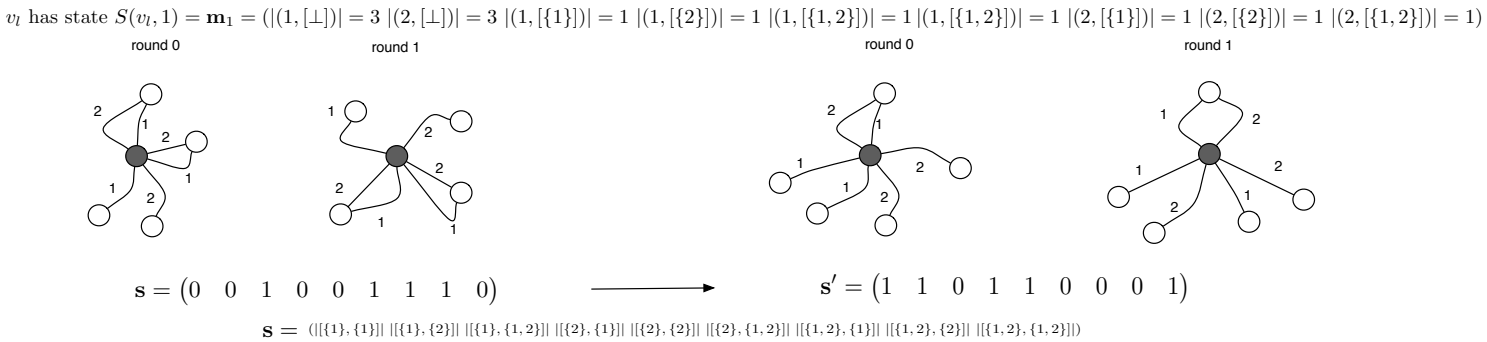


Figure 4: Two dynamic multigraph  $M, M' \in \mathcal{M}(\text{DBL}_2)$  of different size that are indistinguishable at round  $r = 1$ , they induce the same leader state  $S(v_l, 1) = \mathbf{m}_1$ , the relationship among the two is given by the kernel vector  $\mathbf{k}_1$

In order to simplify the proofs, we order columns of  $\mathbf{M}_r$  lexicographically with respect to the state of a process. We consider the following order among elements  $\{1\} < \{2\} < \{1, 2\}$ . As a consequence, the first column of  $\mathbf{M}_r$  will correspond to state:  $|[\{1\}, \dots, \{1\}]|$ , the second column  $|[\{1\}, \dots, \{1\}, \{2\}]|$  and the last one  $|[\{1, 2\}, \dots, \{1, 2\}]|$ . Rows are ordered in the same way. This ordering has been used in Equation 2 and Equation 5. Fixed this ordering we can use a connection  $(j, [x_0, \dots, x_{r'-1}])$



to denote a row  $\mathbf{v} = (\mathbf{M}_r)_{(j, [x_0, \dots, x_{r'-1}])}$  and a node state to denote a single component of a vector, i.e.  $(\mathbf{v})_{[x_0, \dots, x_{r-1}]}$ . Moreover we have that the row vector  $(\mathbf{M}_r)_{(j, [x_0, \dots, x_{r'-1}])}$  will have two trails of ones, with length  $3^{r-r'}$ , for all columns in the form  $[[x_0, \dots, x_{r'-1}, \{j\}, s], [x_0, \dots, x_{r'-1}, \{1, 2\}, s]]$  with  $s \in (\{1\}|\{2\}|\{1, 2\})^{r-r'}$ , and zero for all the other columns (as reference see Eq. 5).

In the following lemmas we specifically characterize the structure of the kernel space of  $\mathbf{M}_r$  in order to identify at which round there is an unique solution.

**Lemma 2.** *Let us consider the matrix  $\mathbf{M}_r$  of the family  $\mathcal{M}(\text{DBL}_2)$  at round  $r$ . The dimension of the kernel space of  $\mathbf{M}_r$  is one (i.e.,  $\ker(\mathbf{M}_r) = \text{SPAN}(\mathbf{k}_r)$ ).*

*Proof.* We first show that rows of  $\mathbf{M}_r$  are linearly independent, thus that the rank of the matrix is equal to the number of rows. The proof is by induction:

- Base Case  $r = 0$ :  $\mathbf{M}_0 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ ,  $\det(\mathbf{M}_0) = 1$  thus the rows are linearly independent.
- Inductive Case  $r$ :  $\mathbf{M}_r$  can be written as  $\mathbf{M}_r = \begin{bmatrix} \mathbf{M}'_{r-1} \\ \mathbf{U} \end{bmatrix}$ , where  $\mathbf{M}'_{r-1}$  is the matrix obtained by  $\mathbf{M}_{r-1}$  substituting each element  $1/(0)$  of  $\mathbf{M}_{r-1}$  with a row vector  $[1 \ 1 \ 1] / ([0 \ 0 \ 0])$ . Now by inductive hyp. we have that all rows of  $\mathbf{M}_{r-1}$  are linearly independent. This implies that also the rows of  $\mathbf{M}'_{r-1}$  are linearly independent, this can be easily shown by contradiction, let us suppose that we have  $(\mathbf{M}'_{r-1})_s = x_a(\mathbf{M}'_{r-1})_a + x_b(\mathbf{M}'_{r-1})_b$  for some rows  $s, a, b$  and two coefficient  $x_a, x_b$ , this means that also if we take the subvectors  $\mathbf{v}^1, \mathbf{v}^2, \mathbf{v}^3$  of  $(\mathbf{M}'_{r-1})_s, (\mathbf{M}'_{r-1})_a, (\mathbf{M}'_{r-1})_b$ , obtained by taking the components in position  $j$  such that  $j \bmod 3 = 0$ , we must have  $\mathbf{v}^1 = x_a \mathbf{v}^2 + x_b \mathbf{v}^3$  but this could be also written as  $(\mathbf{M}_{r-1})_s = x_a(\mathbf{M}_{r-1})_a + x_b(\mathbf{M}_{r-1})_b$  that is clearly a contradiction since the rows of  $\mathbf{M}_{r-1}$  are linearly independent. We now show that a row of  $\mathbf{U}$  cannot be expressed as linear combination of rows of  $\mathbf{M}'_{r-1}$ , we have that the row  $\mathbf{U}_c$  corresponding to connection  $c : (j, [x_0, \dots, x_{r-1}])$ , has only two elements different from zero contained in the subvector  $[1 \ 0 \ 1]$  (if  $j = 1$ ) or  $[0 \ 1 \ 1]$  (if  $j = 2$ ) positioned in the columns with the form  $[x_0, \dots, x_{r-1}, (\{1\}|\{2\}|\{1, 2\})^1]$ . Now, for each row  $(\mathbf{M}'_{r-1})_i$  considering only the values of columns  $[x_0, \dots, x_{r-1}, (\{1\}|\{2\}|\{1, 2\})^1]$ , we get a subvector that is either  $[1 \ 1 \ 1]$  or  $[0 \ 0 \ 0]$ . Therefore it follows that  $[1 \ 0 \ 1]$  or  $[0 \ 1 \ 1]$  cannot be expressed as linear combination of the row vectors of  $\mathbf{M}'_{r-1}$ .

We have to show that the rows vector of  $\mathbf{U}$  are linearly independent. If we consider the sets of 3 columns in the form  $[x_0, \dots, x_{r-1}, (\{1\}|\{2\}|\{1, 2\})^1]$ , only two rows have some elements different from zero: they are either  $[1 \ 0 \ 1]$  or  $[0 \ 1 \ 1]$  that are linearly independent.

This implies, for the rank-nullity theorem [11], that the size of the kernel is  $|\ker(\mathbf{M}_r)| = \text{column}(r) - \text{row}(r) = 3^{r+1} - 2 \sum_{k=0}^r 3^k = 1$ .  $\square$

**Lemma 3.** *Let us consider the matrix  $\mathbf{M}_r$  of the family  $\mathcal{M}(\text{DBL}_2)$  at round  $r$ . We have  $\mathbf{k}_r = [\mathbf{k}_{r-1} \ \mathbf{k}_{r-1} \ -\mathbf{k}_{r-1}]^\top$  with  $\mathbf{k}_{-1} = 1$ .*

*Proof.* The proof is done by induction:

- Base Case,  $\text{round} = 0$ .  $\mathbf{k}_0 = [1 \ 1 \ -1]^\top$  implies  $\mathbf{0} = \mathbf{M}_0 \mathbf{k}_0$ .
- Inductive Case,  $\text{round} = r$ . We assume  $\mathbf{k}_{r-1} = [\mathbf{k}_{r-2} \ \mathbf{k}_{r-2} \ -\mathbf{k}_{r-2}]^\top$ . We show a vector  $\mathbf{k}$  such that its product for the rows of  $\mathbf{M}_r$  corresponding to  $c' = (j, l' : [x_0, \dots, x_{r'-1}])$ , with  $r' < r$  and  $j \in \{1, 2\}$ , is 0. Then we show that the same holds for the remaining rows of  $\mathbf{M}_r$  that corresponds to connection  $c = (j, l : [x_0, \dots, x_{r-1}])$ , and finally we show that  $\mathbf{k} = \mathbf{k}_r = [\mathbf{k}_{r-1} \ \mathbf{k}_{r-1} \ -\mathbf{k}_{r-1}]^\top$ .

Let us consider the row-vector product  $(\mathbf{M}_{r-1})_{c'} \mathbf{k}_{r-1}$  at round  $r-1$ , by definition of kernel we have:

$$0 = \sum_{\forall s \in (\{1\}|\{2\}|\{1, 2\})^{r-r'-1}} (\mathbf{k}_{r-1})_{[l', \{j\}, s]} + \sum_{\forall s \in (\{1\}|\{2\}|\{1, 2\})^{r-r'-1}} (\mathbf{k}_{r-1})_{[l', \{1, 2\}, s]} \quad (6)$$

Let us build a vector  $\mathbf{k} = [(\mathbf{k}_{r-1})_1 \mathbf{k}_0 \quad (\mathbf{k}_{r-1})_2 \mathbf{k}_0 \quad \dots \quad (\mathbf{k}_{r-1})_{3^r} \mathbf{k}_0]^\top$  and let us examine the row-vector product  $(\mathbf{M}_r)_c \mathbf{k}$  :

$$\sum_{\forall s \in (\{1\}|\{2\}|\{1,2\})^{r-r'-1}} ((\mathbf{k})_{|l',(j),s,\{1\}|} + (\mathbf{k})_{|l',(j),s,\{2\}|} + (\mathbf{k})_{|l',(j),s,\{1,2\}|}) + \sum_{\forall s \in (\{1\}|\{2\}|\{1,2\})^{r-r'}} (\mathbf{k})_{|l',\{1,2\},s|} \quad (7)$$

the first term of Eq. 7 can be expressed as follow

$$\begin{aligned} \sum_{\forall s \in (\{1\}|\{2\}|\{1,2\})^{r-r'-1}} ((\mathbf{k})_{|l',(j),s,\{1\}|} + (\mathbf{k})_{|l',(j),s,\{2\}|} + (\mathbf{k})_{|l',(j),s,\{1,2\}|}) = \\ \sum_{\forall s \in (\{1\}|\{2\}|\{1,2\})^{r-r'-1}} ((\mathbf{k}_{r-1})_{|l',(j),s|})((\mathbf{k}_0)_1 + (\mathbf{k}_0)_2 + (\mathbf{k}_0)_3) = \\ \sum_{\forall s \in (\{1\}|\{2\}|\{1,2\})^{r-r'-1}} (\mathbf{k}_{r-1})_{|l',(j),s|} \end{aligned}$$

The second term of Eq. 7 can be rewritten as the first term, then by applying Eq. 6, we have:

$$(\mathbf{M}_r)_{c'} \mathbf{k} = (\mathbf{M}_{r-1})_{c'} \mathbf{k}_{r-1} = 0$$

Now let us consider the row  $c = (j, l : [x_0, \dots, x_{r-1}])$  the row-vector product is  $(\mathbf{M}_r)_c \mathbf{k}$ :

$$(\mathbf{k})_{|l,\{j\}|} + (\mathbf{k})_{|l,\{1,2\}|} = (\mathbf{k}_{r-1})_{|l|}((\mathbf{k}_0)_j + (\mathbf{k}_0)_3) = 0$$

Thus we have  $\mathbf{0} = \mathbf{M}_r \mathbf{k}$ . Now we have to prove that  $\mathbf{k} = [\mathbf{k}_{r-1} \quad \mathbf{k}_{r-1} \quad -\mathbf{k}_{r-1}]^\top$ .

For inductive hypothesis we have  $\mathbf{k}_{r-1} = [\mathbf{k}_{r-2} \quad \mathbf{k}_{r-2} \quad -\mathbf{k}_{r-2}]^\top$ , moreover we have, for Lemma 2, that  $\mathbf{k}_{r-1} = [(\mathbf{k}_{r-2})_1 \mathbf{k}_0 \quad (\mathbf{k}_{r-2})_2 \mathbf{k}_0 \quad \dots \quad (\mathbf{k}_{r-2})_{3^{r-1}} \mathbf{k}_0]^\top$ . This means the first  $3^r$  components of  $\mathbf{k}'$  are  $\mathbf{k}_{r-1}$ , the same holds for the second  $3^r$  components, and the last  $3^r$  are  $-\mathbf{k}_{r-1}$ . This completes the proof.  $\square$

The proof of the following lemma can be found in the Appendix

**Lemma 4.** *Let us consider the matrix  $\mathbf{M}_r$  of the family  $\mathcal{M}(\text{DBL}_2)$  at round  $r$ .*

*We have:* 
$$\begin{cases} \min(\sum^+ \mathbf{k}_r, \sum^- \mathbf{k}_r) = \sum^- \mathbf{k}_r = \frac{1}{2}(3^r + 1) - 1 \\ \sum \mathbf{k}_r = 1 \end{cases}$$

*Proof.* Thanks to lemma 3, we have  $\sum^+ \mathbf{k}_r = 2 \sum^+ \mathbf{k}_{r-1} + \sum^- \mathbf{k}_{r-1}$ ,  $\sum^- \mathbf{k}_r = 2 \sum^- \mathbf{k}_{r-1} + \sum^+ \mathbf{k}_{r-1}$  and  $\sum^+ \mathbf{k}_0 = 2$ ,  $\sum^- \mathbf{k}_0 = 1$ . We first prove, by induction, that  $\sum \mathbf{k}_r = (\sum^+ \mathbf{k}_r - \sum^- \mathbf{k}_r) = 1$ .

- Base case *round=0*:  $\sum^+ \mathbf{k}_0 - \sum^- \mathbf{k}_0 = 1$ .
- Inductive Case *round=r*:  $(\sum^+ \mathbf{k}_r - \sum^- \mathbf{k}_r) = (2 \sum^+ \mathbf{k}_{r-1} + \sum^- \mathbf{k}_{r-1} - \sum^+ \mathbf{k}_{r-1} - 2 \sum^- \mathbf{k}_{r-1}) = (\sum^+ \mathbf{k}_{r-1} - \sum^- \mathbf{k}_{r-1}) = 1$ .

This result leads to the following recursive relation  $\sum^+ \mathbf{k}_r = 3 \sum^+ \mathbf{k}_{r-1} - 1$  for  $\sum^+ \mathbf{k}_r$  with base condition  $\sum^+ \mathbf{k}_0 = 2$ . Solving the recursive relation we obtain  $\sum^+ \mathbf{k}_r = \frac{1}{2}(3^{r+1} + 1)$ . This implies  $\min(\sum^+ \mathbf{k}_r, \sum^- \mathbf{k}_r) = \frac{1}{2}(3^{r+1} + 1) - 1$  where the last term takes into account the fact that the minimum is always the negative component and that  $\sum \mathbf{k}_r = 1$ .  $\square$

From the previous lemma we have:

**Lemma 5.** *Let us consider  $M, M' \in \mathcal{M}(\text{DBL}_2)$  such that their sizes are:  $|W| = n$  and  $|W'| = n + 1$ . Does not exist an algorithm  $\mathcal{A}_l$  that at round  $r \leq \lfloor \log_3(2|n| + 1) \rfloor$  is able to distinguish if it is running on multigraph  $M$  or  $M'$ .*

*Proof.* Let us suppose by contradiction that such algorithm  $\mathcal{A}_l$  exists. For lemma 4 we have  $\sum^- \mathbf{k}_r = \frac{1}{2}(3^{r+1} + 1) - 1 \leq n$ . Let us consider a configuration of non leader processes represented by vector  $\mathbf{s}_r$  with  $\sum \mathbf{s}_r = n$  and such that  $(\mathbf{s}_r)_j \geq 1$  for each  $j \mid (\mathbf{k}_r)_j < 0$  and  $(\mathbf{s}_r)_j = 0$  otherwise. This implies there exists a dynamic multigraph  $M : \{M_1, \dots, M_r, \dots\}$ , of size  $n$ , obtained from  $\mathbf{s}_r$  such that the leader state  $S(v_l, r)$  at round  $r$  is represented by  $\mathbf{m}_r = \mathbf{M}_r \mathbf{s}_r$ . Thus  $\mathcal{A}_l$  outputs  $n$  on the state  $S(v_l, r)$ .

Now let us consider  $\mathbf{s}'_r = \mathbf{k}_r + \mathbf{s}_r$ , by construction we have  $\forall j \mid (\mathbf{s}'_r)_j > 0$  thus  $\mathbf{s}'_r$  represents an instance of dynamic multigraph  $M' : \{M'_1, \dots, M'_r, \dots\}$ , let us denote  $S'(v_l, r)$  the state of  $v_l$  in  $M'$ . Since we have  $\sum \mathbf{s}'_r = \sum \mathbf{k}_r + \sum \mathbf{s}_r = n + 1$ , let us recall that from Lemma 4 we have  $\sum \mathbf{k}_r = 1$ , by hypothesis  $\mathcal{A}_l$  outputs  $n + 1$  on the state  $S'(v_l, r)$ .

But by definition of kernel  $\mathbf{M}_r \mathbf{s}_r = \mathbf{M}_r \mathbf{s}'_r = \mathbf{m}_r$ , thus  $S(v_l, r) = S'(v_l, r)$  therefore  $\mathcal{A}_l$  has to give the same output on the two different instances, that is a contradiction.  $\square$

From the previous lemma and considering that  $\mathcal{M}(\text{DBL}_2) \subseteq \mathcal{M}(\text{DBL}_k)$ , we can state the following theorem whose proof is straightforward.

**Theorem 1.** *Any algorithm  $\mathcal{A}$  cannot solve the counting on an instance  $M \in \mathcal{M}(\text{DBL}_k)$  at round  $r < \lfloor \log_3(2|W| + 1) \rfloor - 1$ .*

From Theorem 1 and Lemma 1 the next theorem immediately follows.

**Theorem 2.** *Given an instance  $G \in \mathcal{G}(\text{PD})_2$  any counting algorithm  $\mathcal{A}$  on  $G$  requires  $\Omega(\log|V|)$  rounds.*

From the previous Theorem we have the following corollary.

**Corollary 1.** *Given a dynamic network with dynamic diameter  $D$ , where  $D$  is constant w.r.t.  $|V|$ . We have that any counting algorithm  $\mathcal{A}$  requires at least  $D + \Omega(\log|V|)$  rounds.*

*Proof.* We create a configuration where  $v_l$  is connected to two nodes  $v_1, v_2$  by a static chain of  $D - 1$  nodes. Nodes  $v_1, v_2$  are connected to the remaining  $\mathcal{O}(|V|)$  nodes mimicking a  $\mathcal{G}(\text{PD})_2$  network. From this observation and Theorem 2 the next corollary follows.  $\square$

**Discussion:** It is interesting to remark how the cost of counting is highly dependent on the information a node knows about the dynamic network (or about the adversary). Let us consider a simplified model where is not possible to have edges among nodes in the same set  $V_h$ , clearly this additional restriction does not impact on the validity of the lower bound and counting in  $\mathcal{G}(\text{PD})_2$  still requires  $\Omega(|V|)$  rounds. However, if we assume that a node  $v$  knows its degree  $|N(v, r)|$  before the receive phase of round  $r$ , as the model considered in [13], then counting in these restricted  $\mathcal{G}(\text{PD})_2$  networks needs  $O(1)$  rounds. The algorithm is trivial: each node in  $V_2$  sends a message  $\frac{1}{|N(v, r)|}$  to nodes in  $V_1$ . A node in  $V_1$  collects these messages and send their sum to the leader. This observation shows how a minimal knowledge on the dynamic graph, e.g., local degree known by a node at the beginning of round  $r$ , may have a great impact on the counting time.

## 5 Conclusion

This paper has shown that on anonymous dynamic networks with constant dynamic diameter there is at least a gap of  $\Omega(\log|V|)$  rounds between counting and information dissemination even considering a model where the bandwidth is unlimited. This difference is actually not present in static networks with IDs, dynamic network with IDs and anonymous static networks. In all these networks, when bandwidth is unlimited, there are algorithms showing that the cost of counting is at most the same order of the dynamic diameter [9, 15, 16]. On the contrary in anonymous networks with broadcast even when  $D$  is constant with respect to  $V$ , we proved that counting is still function of the network size. Solving counting in anonymous dynamic networks with broadcast is still an open problem (see the impossibility result conjectured in [15, 16]) as well as finding a better bound than  $\Omega(D)$  for counting in anonymous 1-interval connected networks without any constraint on  $D$ .

**Acknowledgements:** The work has been partially supported by the Italian PRIN Project TENACE "Protecting National Critical Infrastructures from Cyber Threats".

## References

- [1] S. Abshoff, M. Benter, M. Malatyali, and F. Meyer auf der Heide. On two-party communication through dynamic networks. In *OPODIS 2013*, pages 11–22. Springer, 2013.
- [2] D. Angluin. Local and global properties in networks of processors (extended abstract). In *STOC '80*, pages 82–93. ACM, 1980.
- [3] R. Baldoni, S. Bonomi, A. Cerocchi, and L. Querzoni. Virtual tree: A robust architecture for interval valid queries in dynamic distributed systems. *J. Parallel Distrib. Comput.*, 73(8):1135–1145, 2013.
- [4] M. Bawa, A. Gionis, H. Garcia-Molina, and R. Motwani. The price of validity in dynamic networks. *J. Comput. Syst. Sci.*, 73(3):245–264, May 2007.
- [5] A. Casteigts, P. Flocchini, W. Quattrociocchi, and N. Santoro. Time-varying graphs and dynamic networks. *CoRR*, abs/1012.0009, 2010.
- [6] C. Dutta, G. Pandurangan, R. Rajaraman, Z. Sun, and E. Viola. On the complexity of information spreading in dynamic networks. In *SODA '13*, pages 717–736. SIAM, 2013.
- [7] B. Haeupler and F. Kuhn. Lower bounds on information dissemination in dynamic networks. In *DISC '12*, pages 166–180. Springer, 2012.
- [8] D. Kempe, A. Dobra, and J. Gehrke. Gossip-based computation of aggregate information. In *FOCS '03*, pages 482–491. IEEE, 2003.
- [9] F. Kuhn, N. Lynch, and R. Oshman. Distributed computation in dynamic networks. In *STOC '10*, pages 513–522. ACM, 2010.
- [10] F. Kuhn and R. Oshman. The complexity of data aggregation in directed networks. In *DISC' 11*, pages 416–431, 2011.
- [11] S. Lang. *Linear algebra*. Addison-Wesley Series in Mathematics. Addison-Wesley Publishing Company, 1966.
- [12] G. Di Luna, R. Baldoni, S. Bonomi, and I. Chatzigiannakis. Conscious and unconscious counting on anonymous dynamic networks. In *ICDCN '14*, pages 257–271. Springer, 2014.
- [13] G. Di Luna, R. Baldoni, S. Bonomi, and I. Chatzigiannakis. Counting in anonymous dynamic networks under worst case adversary. In *ICDCS '14*, pages 338–347. IEEE, 2014.
- [14] E. Le Merrer, A.-M. Kermarrec, and L. Massoulie. Peer to peer size estimation in large and dynamic networks: A comparative study. In *HPDC '06*, pages 7–17. IEEE, 2006.
- [15] O. Michail, I. Chatzigiannakis, and P. Spirakis. Brief announcement: Naming and counting in anonymous unknown dynamic networks. In *DISC '12*, pages 437–438. Springer, 2012.
- [16] O. Michail, I. Chatzigiannakis, and P. Spirakis. Naming and counting in anonymous unknown dynamic networks. In *SSS '13*, pages 281–295. Springer, 2013.
- [17] R. O'Dell and R. Wattenhofer. Information dissemination in highly dynamic graphs. In *DIALM-POMC '05*, pages 104–110. ACM, 2005.
- [18] M. Yamashita and T. Kameda. Computing on an anonymous network. In *PODC '88*, pages 117–130. ACM, 1988.